

Signing the Root

A Nominet position paper

Contents

1. Introduction.....	1
1.1 A key point in time.....	1
1.2 Who needs DNSSEC anyway?.....	1
1.3 What comes after DNSSEC?.....	2
2. DNSSEC, the basic purpose.....	2
2.1 The impact of DNSSEC on delegation-only zones.....	2
2.2 What does it mean when someone signs a delegation-only zone?.....	2
3. The challenges of implementing DNSSEC.....	3
3.1 The chain of trust.....	3
3.2 Secure key management.....	3
3.3 Signing changes.....	3
3.4 Automated re-signing.....	3
3.5 Managing resource usage.....	3
4. Signing the root.....	3
4.1 Why is it important to sign the root?.....	4
4.2 What are the options for signing the root?.....	4
4.3 How it should work?.....	4
4.4 Interplay with Internet Governance.....	5
5. Is there an alternative to signing the root?.....	5
6. Our proposals in brief.....	5
7. Glossary.....	5

1. Introduction

In this paper we examine the issues currently preventing widespread adoption of DNSSEC with a special focus on the issues involved in signing the root zone. After considering the pertinent concerns, we suggest a solution to signing the root that we believe balances the requirements of all concerned.

1.1 A key point in time

DNSSEC is currently not widely deployed, as there are a number of unresolved issues, both technical and political, which are limiting its deployment.

Until now, the major barriers to technical implementation have been:

- Zone-file enumeration
- Support for DNSSEC in application software
- The impact on resources of fully signing a large zone.

These barriers are close to being overcome, thanks in part to the input of Nominet through the Internet Engineering Task Force (IETF), with the imminent approval of improvements to DNSSEC called NSEC3.

The resolution of outstanding technical issues focuses attention on another key step which must be completed prior to the successful implementation of DNSSEC: the signing of the root zone, the so-called "trust anchor".

In this paper, we provide our solution for overcoming this remaining barrier to the widespread adoption of DNSSEC.

1.2 Who needs DNSSEC anyway?

It is clear that DNSSEC has not captured the public imagination. End users of DNS are not raising a clamour for the introduction of DNSSEC. However, this should not lead to a misapprehension that DNSSEC is not needed or wanted.

There is a significant desire amongst all Internet users including government, industry and civil society for a more secure and trustworthy Internet. It is clear that this will only be achieved by a combined approach of multi-layered technical developments and multi-layered policy developments.

The received technical wisdom is that a secure DNS is a fundamental layer in that technical development, on which many other layers depend. But it is a layer of technology that many are unaware of and will remain so, even while the public embodiment of DNS, domain names, remain a high profile concern.

It is our view that it is imperative for TLD registries to lead the implementation of DNSSEC, raising awareness amongst other users of DNS, with the aim that a secure DNS becomes a ubiquitous feature of the Internet.

1.3 What comes after DNSSEC?

Once implemented, DNSSEC will provide very real benefits. When errors can be detected, what is left is a highly trustworthy distributed database, which will provide a secure foundation for many of the new uses of the DNS.

One good example is Domain Keys Identified Mail (DKIM). This is a technology that adds cryptographic signatures to emails, to prevent address spoofing and utilises the DNS to publish the keys for signature checking. With DNSSEC securing the delivery of those keys, the effectiveness of DKIM is increased and the techniques available to distributors of spam are reduced.

2. DNSSEC, the basic purpose

It is important to remember that DNSSEC was designed to protect Internet users from security threats such as DNS cache poisoning – the introduction of fake DNS data into caching DNS servers, and so-called ‘man-in-the-middle’ attacks – supplying fake data that usurps genuine responses to DNS queries.

DNSSEC provides protection by enabling a computer to check whether the information contained in a given DNS response has come from a trusted source and whether it has been tampered with in transit.

DNSSEC is essentially error detection, where the ‘error’ could be introduced by a malicious entity, which without DNSSEC would remain undetected.

2.1 The impact of DNSSEC on delegation-only zones

The zones managed by TLDs are normally delegation-only. That means that they contain only nameserver records that delegate domains down the DNS hierarchy.

The normal registry process is for the TLD to receive the nameserver data from the owner of the sub-domain, possibly to run this through some checks before accepting the data, and then to publish it in the TLD zone.

With DNSSEC this model will change slightly as the TLD will additionally need to receive the key identifiers needed to construct Delegation Signer (DS) records. The TLD will then sign the DS record and now publish the nameserver data, the key identifier for the child zone and the TLD signature of this key identifier.

It should be noted that the delegation nameserver data is not signed in DNSSEC because the parent zone is not deemed to be authoritative for the nameserver data, only the child can authoritatively publish its own nameservers.

2.2 What does it mean when someone signs a delegation-only zone?

In this context we examine what it means when a TLD signs a delegation data. It could either mean:

1. We are using the signature to warrant that we have checked the delegation data we are publishing and it can be trusted; or
2. We are using the signature to transmit securely the delegation data supplied to us, but make no warranty as to the trustworthiness of the data.

In our view, wherever a zone is situated in the DNS hierarchy, the meaning of signing a zone should be consistent across the DNS. In other words, we would not make any requirements on the root zone, or our users, that we ourselves were not prepared to meet.

For any zone where the owner of that zone is different from the owner of the parent, the parent would be unable to guarantee the truth of statement (1) above. This is the position of all TLD managers as they are not the owners of the zones for the domains they delegate and so they could not guarantee the truth of statement (1).

Statement (2) is consistent with the DNSSEC standard, which was developed with the limited purpose of enabling secure transmission of DNS data.

Therefore, the entity that signs delegation data in a zone makes a limited promise: that the data received is the same as the data published within the relevant zone.

It should be noted that this is exactly the promise currently made by the publishers of delegation data in zones, but without DNSSEC they cannot transmit that data securely.

3. The challenges of implementing DNSSEC

The implementation challenges remaining to us can be summarized as:

- the chain of trust
- secure key management
- signing changes
- automated re-signing
- managing resource usage

3.1 The chain of trust

In order for DNSSEC to be fully deployed, an unbroken chain of trust needs to be established, down from the root at the top, through the TLD, down to individual registrants. All zones need to be authenticated by “signing”, i.e. the publisher of a zone signs that zone prior to publication and the parent of that zone publishes the keys of that zone.

To achieve this we need the root signed and procedures in place at each step to enable the secure transmission of keys between parties.

3.2 Secure key management

Currently registries only make minimal use of keys within DNS transactions as part of the ordinary operations of the registry. Managing DNSSEC keys requires a registry to implement a new infrastructure for the secure storage and transmission of keys, including both suitable equipment and procedures.

3.3 Signing changes

In common with a few of the larger TLD registries, Nominet currently provides near synchronous zone file publication. This means that new domain name registrations are entered into the DNS within minutes and can work almost immediately.

Signing a large zone, like co.uk which has over 6 million registrations, would be a highly involved and maintenance-intensive task. Given the frequency of updates to the records within co.uk, which can peak at 300,000 per day, signing a large, fast-changing zone in real time will require significant cryptographic processing power and reliability.

3.4 Automated re-signing

With any zone it is likely that the signatures will expire before the DNS records are updated. Zone operators therefore require a means to automatically re-sign DNS records before these signatures expire. This functionality is dubbed ‘continuous signing’ and is not yet a feature of common nameserver implementations.

Nominet is therefore providing financial assistance to the Internet Standards Consortium (ISC) to fund the development of continuous signing within BIND, one of the most popular nameserver implementations in deployment.

3.5 Managing resource usage

Signed DNS records are considerably larger than unsigned records, with a fully signed zone being an order of magnitude greater in size than an unsigned zone. Some registries have expressed concern at the impact this will have on their infrastructure and possibly limit their involvement with DNSSEC as a consequence.

However a solution for this exists with NSEC3, the enhancements to DNSSEC that are close to becoming an RFC. This solution is called ‘opt-out’ and enables a zone operator to only sign those delegations that need DNSSEC. A registry that uses this can manage the increase in resources in line with the gradual uptake of DNSSEC, rather than being forced into an all-or-nothing upgrade.

Traditional capacity management for registries has been based around the number of domains within the zone. However, future capacity planning will need to incorporate the additional factor of the number of signed zones to ensure that a true picture of resource requirements is developed.

4. Signing the root

The IANA root zone is both the authoritative list of TLDs and the starting point for delegation data to locate those TLDs. Without a single point (the root), the world would have to find TLD locations individually, without using the DNS and without any certainty that the TLDs were genuine. This clearly does not scale and is intensive and potentially error prone.

Although a single root is not a technical necessity, it is the Nominet view that, in practice, it is essential for the stability of the Internet.

The DNS root database is managed by ICANN through the IANA function. IANA staff are responsible for updating the database of TLD managers. Currently, each update that is made to the DNS root database is reviewed by the US Department of Commerce prior to going live. This function has caused substantial debate at the international level, particularly during and after the World Summit on the Information Society.

Once the root database has been updated, the data that needs to change in the root zone is sent to the Root Zone Manager (RZM), currently Verisign Inc., who then propagates this through the Internet to the other root server operators.

4.1 Why is it important to sign the root?

DNSSEC requires a trust anchor to work. That is, a point in the DNS hierarchy that a DNS user explicitly trusts and from which they can start the chain of trust that continues down the hierarchy.

Without a single origin of trust, those wishing to use DNSSEC would need to identify multiple trust anchors and monitor them continuously. Again this does not scale and is intensive and potentially error prone.

Experience shows that for successful deployment of new technology, end-users should be required to do very little. In this case, the system administrators around the world who configure DNS servers should be able to make them use secure DNS as simply as possible.

For this to happen, we contend that there should be a single trust anchor and that this should be at the same point as the single authoritative list of TLDs. This can only be achieved by signing the root. Indeed, the standard has been designed on this assumption. Anything else would be splitting the root.

Whilst a number of registries have pioneered the deployment of DNSSEC by signing their own zones and establishing themselves as trust anchors, this is not a stratagem that can be extended beyond these early adopters. As explained before, using multiple trust anchors does not scale and is likely to inhibit the growth of DNSSEC rather than promote it by making the management of DNSSEC too complex.

We therefore recommend that any TLD considering signing its zones and becoming a trust anchor, carefully weighs the wider implications of participating in a mechanism that does not scale.

4.2 What are the options for signing the root?

The identity of the organization or entity that signs the root has been troubling the Internet community for some time. Several options are currently under discussion within the community:

- The current manager of the root zone – the IANA
- The outsourced Root Zone Maintainer, Verisign Inc.
- A trusted third party

In order to evaluate the options, we consider the relevant factors:

- Although the root zone is relatively stable, and does not have nearly the same volume of ongoing updates that affect larger zones (eg .co.uk), implementing DNSSEC will bring a higher degree of complexity and technical maintenance to management of the root zone than previously.
- The consequences of errors in signing a zone could be severe, but are no worse than the current consequences of a mistake in managing the root zone data.
- Even with relatively stable data, there will be a need for signatures to be replaced regularly and so generate a far higher volume of changes to the root zone than there is currently. This signature rollover needs to happen on a regular basis, regardless of how often the root zone is updated with regular DNS changes.
- To introduce an unrelated third party would potentially add delay, cost and complexity, and thereby inhibit DNSSEC take-up.

4.3 How it should work?

From our analysis of these factors, we believe that the following proposal is the best possible solution to this apparently intractable problem.

IANA should be responsible for creating and maintaining the Key Signing Keys (KSKs) used for the root zone. IANA and IANA alone should have the private portions of the keys and use those for the generation of Zone Signing Keys (ZSKs).

IANA should send to the RZM the public portions of the KSKs and the public and private portions of the ZSKs for the RZM to use.

The RZM should be responsible for publishing the public portions of both keys in the root zone and for using the ZSKs to create signatures following agreed algorithms that maintain the balance between security and manageability.

We believe this maintains the appropriate balance of security and practicality of implementation, whilst reflecting the current separation of responsibilities between IANA and the RZM.

To be clear, we do not believe there is any role for a third party in this process.

4.4 Interplay with Internet Governance

Whilst we are aware that the role of IANA, and in particular the role of the US Department of Commerce in reviewing each zone file update, has provoked international controversy for example during the World Summit on the Information Society. Mechanisms incorporated into the Tunis Agenda, such as the process towards enhanced cooperation, together with ongoing discussions within the Internet Governance Forum, should incorporate the expanded root management function, including DNSSEC signing.

Our proposal would not alter (or strengthen) the role currently undertaken by the US Government. It would leave day-to-day technical management in the hands of a technical body.

5. Is there an alternative to signing the root?

Without a signed root, each Top Level Domain that enables DNSSEC will have to arrange for the distribution of their trust anchor to security-enabled nameservers worldwide. A scheme called DNSSEC Lookaside Validation (DLV) has been proposed as a way of doing this.

Theoretically, the concept of DLV side-steps the issue of "who signs the root" by creating an authentication point at an unrelated part of the DNS hierarchy. Furthermore DLV can support multiple points of validation across the DNS.

However, we believe that DLV should not be considered a credible alternative to signing the root, for the following reasons:

- We believe that a trust anchor root that is separate from the authoritative TLD root introduces a level of complexity that is too much for widespread public adoption. There are questions of how TLDs are to be authenticated into a DLV root, who is responsible for it and which of many DLV roots is the right one to trust.
- DLV is technically problematic. It requires a high level of traffic to the DLV root and a dependency on the DLV root being available at all times. Widespread adoption of DLV would therefore introduce fragility to DNS that has never existed before. It is widely accepted that the robustness of DNS has been a major contributor to its success and DLV in its current form could undermine that.

It should be noted that DLV is not a standard and is unlikely to become one whilst it remains technically problematic.

We are working with others on an alternative DLV proposal that would fix the technical problems with DLV, but still would not make DLV an alternative to signing the root.

6. Our proposals in brief

- There should be a single root that combines the authoritative list of TLDs and the start of the DNSSEC chain of trust for those TLDs.
- Sign the root as soon as possible, with IANA responsible for creating and managing keys and the RZM responsible for adding signatures to the root zone data.
- Deal with oversight issues for the IANA function as a whole, through the ongoing process towards enhanced cooperation arising out of the Tunis Agenda.
- Avoid DLV.

7. Glossary

BIND

The Berkeley Internet Name Daemon is the most common DNS nameserver implementation in use worldwide. Whilst BIND is open source, it is developed and maintained by the Internet Systems Consortium, a highly professional and capable organisation who make BIND available for multiple platforms and languages. Recognising the importance of BIND to our work, we are a major contributor of fund to ISC for the ongoing support and development of BIND.

DKIM

Domain Keys Identified Mail is a technology that allows a cryptographic signature to be added to outgoing emails, thereby allowing the recipient to verify they were genuinely sent from the address that is given as the sender in the message. Without DKIM spammers will continue to be able to send email where the sender address has been faked and the recipient will be unable to detect this through automated means.

DLV

Domain Lookaside Validation, is a scheme to publish trust anchors for zones, outside of the Domain Name System's hierarchy, hence the term 'lookaside'. This allows for aggregation of TLD trust anchors on various locations, avoiding the necessity to have a single signed root.

KSK and ZSK

A Key Signing Key is a fundamental component of DNSSEC. This is a cryptographic key that is used solely to sign other keys as part of a chain of trust.

A Zone Signing Key is a key used to sign the data published in a zone. A ZSK is signed by a KSK and is generally a shorter lived (and possibly cryptographically weaker) key than a KSK.

By splitting the usage of keys between KSKs and ZSKs a balance is made between the processing required to verify a signature, the lifetime a key is in use, and the frequency with which a user of the zone needs to retrieve and verify new keys.

NSEC3

An enhancement to DNSSEC that changes the way answers on non-existent or insecure delegations are given. It prevents the practice of zone file enumeration, where a miscreant can use NSEC records (the precursor to NSEC3) to gain an entire copy of a zone file remotely. NSEC3 also adds support for opt-in, whereby a zone publisher can choose whether insecure delegations are signed or unsigned.

RZM

The Root Zone Maintainer (RZM) is the organisation contracted to manage updates to the root zone and to distribute those to the root server operators. The RZM at the time of writing is Verisign.

TLD

A Top Level Domain is a domain immediately below the root, such as .uk or .com.